International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

Image Forgery Detection Techniques Used In Forensics

Anushka Darade[1], Dhairya Umrania[2], Jaansi Bhansali[3], Utsav Parekh[4]

[1]Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India
[2]Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India
[3]Student, Dept. of Life Sciences, Jai Hind College, Maharashtra, India
Student, Dept. of Information Technology, K. J. Somaiya College of Engineering, Maharashtra, India

---

Abstract - *Nowadays, anyone can easily forge a digital image and it becomes difficult for naked eye to differentiate the original image and the forged image. Digital image forensics is one such field of study that helps to verify the authenticity and integrity of images. The paper presents a literature review of image forgery detection techniques such as copy move forgery detection - keypoint based method and block based method, detection by color contrast, control based image forgery detection and Support Vector Machine. The authors of the paper have given a brief description of these techniques with comparison tables, accuracy, graphics and algorithms.*

Key Words: Copy Move Forgery, Forensics, SVM (Support Vector Machine), SIFT (Scale Invariant Feature Transform), Keypoint matching, Block based matching methods, RGB, contrast

1. INTRODUCTION

We live in a world where digital media is constantly on the rise and we're surrounded by it. This digital media can be in the form of messages, voice recordings, images, videos, GIFs etc. They are a key part of our day to day lives which are used to portray the world around us. Although, at times they can also be used to deceive others. With all the latest tools and technologies available, it is possible to edit and tamper an image which can be used for malicious purposes. In forensics this can lead to many problems, such as forged evidence, false accusations, incorrect conclusions and so on. It is imperative to find out whether an image is forged or not. In this paper we will look at a few of the techniques which are used in forensics to detect image forgery.

Forgery can be of many types, one common type is Copy - Move Forgery where the perpetrator copies objects from images to places where those objects shouldn't be. More about copy move forgery is discussed further in the paper. We will look at several techniques used in forensics which can be used to detect copy - move forgery.

In the paper we have explored a total of 5 techniques used to detect forgery. In the first section the authors cover Key-Point matching technique and Block based matching technique and how they are used to detect copy move forgery. After that, in the second section the authors explore techniques which can detect image forgery in general and can also be applied to copy-move forgery. This section contains algorithms which show how color schemes and color patterns of an image can be utilized to detect forgery, mainly we have covered two properties of images in this, which are: the pixel color scheme values such as RGB values, etc. and the contrast levels of images. In the last section the authors have looked at how to use SVMs, a famous machine learning algorithm, to detect forgery.

2. Copy Move Forgery

Copy move forgery (CMF) detection has mainly two approaches: Keypoint based methods and block based methods. Compared to keypoint based methods, block based methods have higher processing costs due to large blocks of data. This method fails if a region has undergone geometric transformation. On the other hand, key-point based methods have an advantage over block based methods, it fails when the tampered region occurs in a low entropy region of the picture.

2.1 Key-Point Matching

The authors will be discussing different Key-point matching techniques to detect copy-move forgery. One very good algorithm used is SIFT (Scale Invariant Feature Transform). This algorithm is very robust and works even when there are rotations and escalations of objects. In this section we'll be covering 2 methods which utilize SIFT to detect copy-move forgery [5].

- **SIFT-Point Matching Method:**

This method uses SIFT descriptors to match and detect similar pixels of an image. It uses Euclidean distance as a similarity measure between 2 SIFT descriptor vectors. This method has good performance but it also has a few drawbacks. Since we're matching pixel to pixel, many similar but different pixels are matched together, and some distinct but same pixels are not matched. Hence this method is good but it leaves room for improvement [5].

- **SIFT-Point Cluster Matching:**

In this method instead of taking SIFT descriptor vectors of points, points are first clustered into objects, which are then compared with other similar objects. This method provides massive improvement to the previous method as shown by Fig 1.

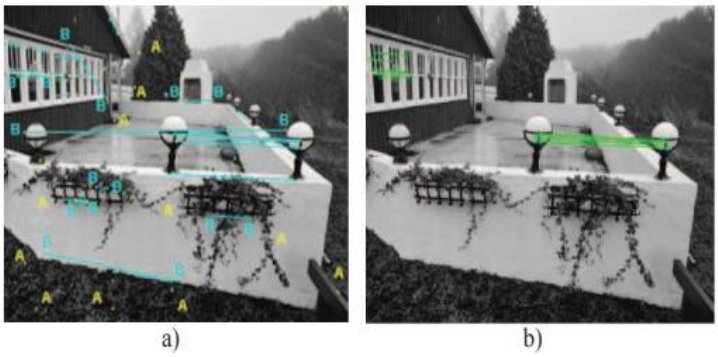


Fig -1: The lamp on the center is a copy of that on the right. Results after keypoint matching a) and cluster matching b). Much less false positives are detected in b) (only the two windows, which have a very repetitive structure). Note that in b) the other lamps in the image (not copies) are correctly not detected.

The first step is to compute the SIFT descriptors for each point in an image. Then the points are to be clustered, E. Ardizzone, A. Bruno and G. Mazzola, have used Agglomerative Hierarchical clustering as the clustering algorithm in their paper[5].
Once the clustering is done, we have grouped the pixels together to identify an object. Now we'll start matching clusters, instead of points, which are basically comparing objects or patterns irrespective of the scale or rotation in them. Instead of using Euclidean distance for this step, this paper has preferred to use Cosine distance to compute the angle between two vectors to find matches.
E. Ardizzone, A. Bruno and G. Mazzola showed through experimental results in paper [5], SIFT-point matching technique gave 44% precision which was increased to 72% after parameter tuning, but SIFT-point Cluster matching method gave 92% precision.

- **KLSP (Key Point Localized Super Pixel):**

C. Rajalakshmi, M.G. Alex and R. Balasubramanian, propose a method in [4], which uses SIFT along with another algorithm: LRW, and by experimentation, it claims it has proved to have a better performance than previous methods. The method is called KLSP (Key Point Localized Super Pixel). This method is depicted in Fig 2. [4]

How KLSP method works:

This method uses LRW method to get segmented pixels which are known as Super Pixels. These super pixels are used as the key-points used in SIFT algorithm and the super pixels are compared to detect copy-move forgery. The full algorithm is mentioned in the image below:

Algorithm proposed for KLSP in [4]:

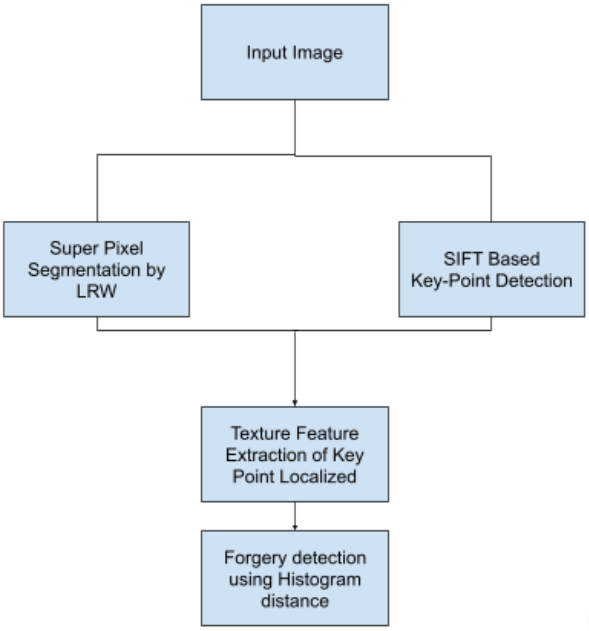


Fig -2: Outline of the key point localized super pixels (KLSP) method

Step 1: I, Input image //Let '*I*' be the input Image

Step 2: Apply LRW to '*I*' //Apply LRW algorithm to the above image to find out super pixels.

Step 3: Find Super pixel $I_{(sup)}$ for *I*

Step 4: Find Key points (K_p) for the image *I* using SIFT Algorithm

Step 5: Create Fake list 'FList' Let FList = φ

Step 6: for each $k_{p(i)}$ ε *Kp* find Texture features LBP for the super pixel in which $k_{p(i)}$ occur

Step 7: for *i* = 1 to ||Kp||–1 for j = *i*+1 to ||Kp||

Step 8: Find Chi-square Histogram distance d_{ij} = chisquare (Hist(*kpi*) , Hist(*kpj*)

Step 9: If d_{ij} < Threshold then Forgery occurs.

Step10: $F_{List} = F_{List} \cup kp_i \cup kp_j$ Add Super pixel region i & j to fake list 'F_{List}'.
End

Step11: If F_{List} = φ, then Forgery not found.
else
Forgery is found.

Experiment results:

C. Rajalakshmi, M.G. Alex and R. Balasubramanian experimented in [4] with several algorithms such as SURF, PCA + SIFT, DWT + SIFT, but LRW + SIFT (KLSP) had the highest sensitivity at 98.18%, highest specificity at 93.64% and the highest accuracy at 93.64%. Hence, LRW+SIFT, which is KLSP, has the best results compared to the other algorithms. [4]

2.2 Block-Based image forgery detection Algorithms

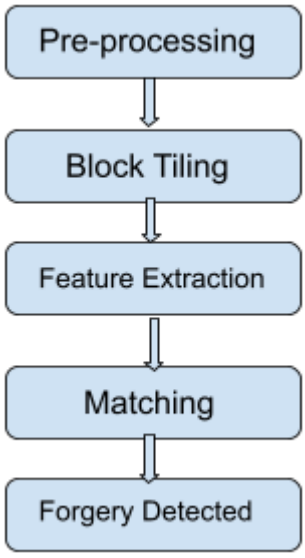


Fig -3: Steps for Copy Move Forgery Detection Algorithm [10]

Steps followed in block-based for Copy Move forgery detection are as follows [13]:

A. Pre-processing - It is the first and optional step for copy move forgery detection. Colored images can be converted into grey-scale images to reduce size of image. Some images might require preprocessing, some might not. But it is preferred to do pre-processing, so that processing becomes fast.

B. Feature Extraction - An image is divided into blocks as part of the block based method, which is termed as block tiling.

For an image size of M × N and a block n size of bxb, the number of overlapped blocks is given by (M-b+1) x (N-b+1). After block tiling features are extracted from each block [10]. Features like Local binary pattern, discrete cosine transform (DCT), discrete wavelet transform, and Principal Component Analysis (PCA) etc. are used in block based methods as explained below:

1. **Discrete Wavelet Transformation (DWT)** DWT is the technique which can help in reducing the size of the image at each level. The primary purpose of the Wavelet transform is to decompose a signal into a fixed basic function. These features are known as wavelets. Mother Wavelet is defined as the wavelets which are procured from a single model wavelet by shifting and dilation. DWT breaks the signal into low and high-frequency parts. The low frequency contains the raw information of the signal, and the high-frequency part abides by the information regarding the edge components.
2. **Principal Component Analysis (PCA)** One of the statistical methods is PCA, which comes under feature extraction. PCA has the main purpose of reducing the dimensionality, which helps in describing the data more economically. This requires a strong correlation between observed variables. It is considered as a successful method which helps in image recognition and reduction.
3. **Discrete Cosine Transform (DCT)** One of the prominent image compression methods is DCT. It has a wide range of applications for image compression for JPEG and compression for videos in MPEG. MJPEG, DV. In DCT, computation is done in 2-dimensional blocks and we get results in quantized format.
4. **Singular Value Decomposition (SVD)** It is the orthogonal matrix decomposition technique which is reliable and robust. SVD has become widely used in the signal processing area. SVD in layman terms is an alluring algebraic transformation for processing in images.
5. **Local Binary Pattern (LBP)** LBP labels the pixels of an image by segmenting the neighbouring pixels and converting them to binary numbers. LBP texture operator is favoured by many applications because of its processing simplicity and discriminative power.

C. Matching - Matching helps to detect the twin regions in image forgery detection. High percentage of matching or similarity between 2 features is interpreted as admonitory for a duplicated region. Methods used for matching can be lexicographic sorting, Best-Bin-First search etc. Block Based copy-move forgery detection method uses following types of matching methods:

1. **Robust Match:** The idea of exact matching is used in this method. We extract the blocks which are an exact match. We can also use the function to find the exact pixel values of blocks. Next we extract uncommon blocks. Later these features are used to detect copy move forgery by matching the features.
2. **Euclidean Distance:** the Euclidean distance is the difference between two pixels calculated by the Euclidean distance formula.
3. **K-D tree:** The closest point search in high dimensional KD-trees is closely related to nearest neighbour search in a low dimensional projection,

and that the long tail of the probability distribution p(n) is a major reason why searching in a single KD-tree[14] will fail, whereas using several KD-trees with independently rotated data will work much better.

D. Forgery detected - After paired forged regions are detected. Forged regions are marked so that users can see the forged areas. In the table below, the authors have discussed various block based copy move forgery algorithms. The advantages and disadvantages of each of these methods are discussed in the comparison table. It helps for easy comparison of different methods to use.

Table -1: Comparison of different Block-based Copy move forgery detection algorithms

Feature Extraction Method	Method for matching	Advantages	Disadvantages
DCT	Autocorrelation	It can easily detect a forgery when the image is stored in lossy format.	Human monitoring is required.
PCA	Row distance	Helps in reducing dimensionality. Works well in presence of noise.	Does not work efficiently on small sized blocks.
LBP	Euclidean distance	Powerful over blurring and flipping of image.	Cannot identify forgery regions with rotated angles.
SVD	kd-tree, Euclidean distance	Easy to use.	Cannot identify pasted and copied parts of image.
Zernik moments	Euclidean distance	Works excellently against AWGN, JPEG and blurring.	Doesn't work well against Affine transformations.

3. Detection of image forgery using color constancy.

The use of color image processing to identify forgery is dependent on the fact that color is a powerful description tool and that it simplifies the extraction and identification of an object from the scene. When light is achromatic it's only characteristic can be its intensity or the amount of the light .It basically describes a black and white picture hence introducing us to the term gray level, referring to a scalar measure of intensity that ranges from black, to grays, and finally to white. But what if the image is not black and white? In that case one can be introduced to multiple color models. These color models are a way to specify colors in a more standardised and generalized manner [19]. A color model is a representation of a color in the coordinate system. It is the simplest way to describe a color and how it'd be used in a computer model. The color Model is representing each color as a coordinate.

In terms of digital image processing, the hardware-oriented models most commonly used in practice are the RGB (red, green, blue) model for color monitors and a broad class of color video cameras; The CMYK (cyan, magenta Yellow, Black) model is used for color printings and the HIS model (hue, saturation, intensity) corresponds closely with the way humans describe and interpret color [19].

3.1 HIS Color Model

The HIS color model focuses on the intensity part of the colored image, this helps in describing the color on bases of the amount of light depicted in the image. It is an ideal tool for developing algorithms that are naturally seen by the human eyes who at the end develop these algorithms.

3.2 RGB Color Model

In the RGB color model each color appears as a combination of the primary spectral component Red, Green and Blue. It is a model that is based on the Cartesian coordinate system where in the color subspace of interest is a cube.[1] RGB values are at three corners; cyan, magenta, and yellow are at three other corners; black is at the origin; and white is at the corner farthest from the origin [2].The image represented in this model has a component images for each of the three primary colors, once fed into the RGB monitor each of the three images are said to combine on the phosphor screen to produce a composite color image[2]. The number of bits that are used to exhibit each of the pixels in the RGB space is called the pixel depth of the image.

3.3 Proposed Forgery detection method by RGB Model

This method was proposed by Kasban, H., & Nassar, S.in their paper [1]. An efficient approach for forgery detection in digital images using Hilbert Huang transform.
This method consists of 4 steps namely:

A. Conversion of RGB image into YCbCr color space.

Most of the images to be tested come in the form of 2D RGB images. The human eye having a different sensitivity to color and brightness makes the conversion of the RGB image into a YCbCr image for forgery detection. The components of YCbCr are as follows: Luminance Y, Chrominance Blue Cb, and Chrominance Red Cr. Luminance is like the grayscale image, which describes image content and it is more sensitive to the

human eye than the chrominance components. Cb is strong in the case of image parts containing the sky (blue), and Cr is strong in places of occurrence of red colors.

B. Extraction of the HHT features from the chrominance-red component Cr.

The Hilbert–Huang Transform usually consists of 2 stages where in the first stage would be to decompose the image into Intrinsic Mode functions using the Empirical Mode Decomposition (EMD)where each part of the forged image is actually considered to be a part of the real image. In the case of forgery detection the Red chrominance which is a 2 dimensional component is broken down into a one-dimensional signal followed by a second stage where in the decomposed data is used in the spectral analysis. And the second stage is the spectral analysis using Hilbert spectral analysis. Finally the mean, the variance, the skewness and the kurtosis of the first 4 IMFs' amplitude spectrums and instantaneous frequencies is calculated to obtain a sum of 32 features [2].

C. Classifying between the authentic images and the forged images using classifiers.

Machine learning is a method in which a machine learns about a prior model and helps in predicting futuristic outcomes. It is based on the learning by artificial intelligence and can be induced using many different statistical, probabilistic, and optimization techniques such as logistic regression, artificial neural networks (ANN), K-nearest neighbor (KNN), decision trees (DT) Support Vector machine (SVM) and Naive Bayes. The SVM, ANN or KNN classifiers are proposed to be able to achieve high accuracy [2].

D. Verifying the classified results and calculating the detection accuracy.

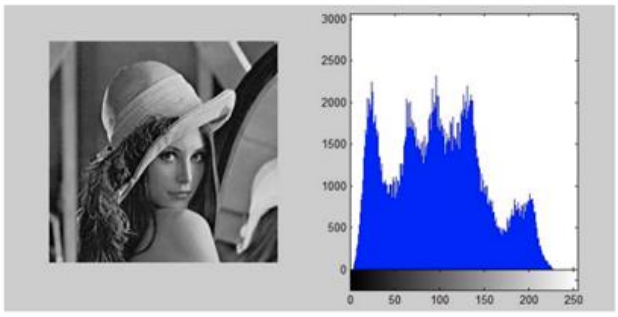
The results after classification should be verified by comparing the detection accuracy. This can be done using SSIM. Another method such as cross correlation also could be used

4. Contrast Based Image Forgery Detection

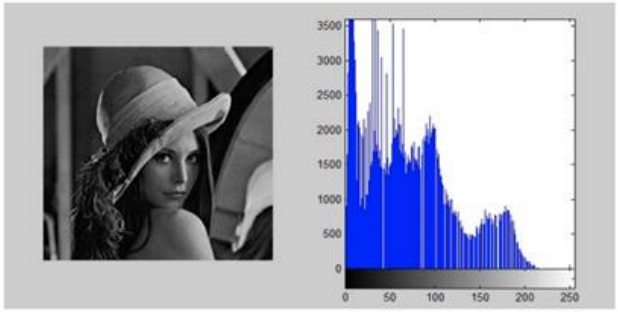
When someone has forged an image, the contrast of that image is affected. In this section the authors discuss the ways in which a forged image can be detected based on detection of contrast enhancements.

First, we'll understand what contrast is. Contrast is the degree of difference between two objects, and in images, pixels. We can plot the histogram of the intensity of each pixel to see how the distribution of pixels looks. Next, we'll look at how this will help in detecting forged images. When we have a typical copy-paste forgery, in that the copied image's contrast does not align with the contrast of the other image. This irregularity of a pattern can be used to identify a forged image. Many perpetrators know about this and try to cover it up, but instead it exposes them further. The authors will explore next, how it exposes them.[6]

The different degrees of intensity of each pixel can be mapped on a Histogram. This histogram helps us identify the contrast level of the image because it shows us the distribution of different pixel intensities. There are many properties of contrast which can be gauged from this histogram, and those properties can be used to determine whether an image is forged or not. In Fig 4., the difference between a normal image's and when its contrast is changed, both histograms are shown.



(a)



(b)

[9]

Fig -4: (a) Original images and its histogram and (b) Contrast changed image and its histogram

One property that is affected by forgery is the peaks and zeros of the histogram are the peaks and zeros of the histogram which can clearly be seen from Fig. 4. Therefore, this can be used to create a high frequency measurement "F", and a threshold can be set "η". If F is greater than η, we can conclude the image has been tampered with contrast enhancement. [6]

There are several techniques used to identify forged images using contrast enhancement detection techniques, we'll be discussing 3 of them.

4.1 Peaks/bins method of identification contrast enhancement in [6]:

We can identify using the peaks and bins of the image histogram. This is also called histogram method. Steps are as follows:

• Step 1. Create the histogram of the image and evaluate the modified histogram, g(x) = h(x)p(x), where x is original value of pixel, and p(x) is known as pinch off function, which eliminates extremes of saturation in the histogram, basically makes it smooth.

if (xNp):
    p(x)=12 1-cos(xN)
else if (x255-Np):
    p(x)=12 1+cos(x+Np-255)Np
else:
    p(x)=1

Np is the width of the histogram spectrum where p(x) decreases from 1 to 0. Normally it is fixed at 8.

• Step 2. g(x) is transformed into the Fourier frequency transform domain, G(k), and then we calculate the high frequency measurement F based on t.

F=1Nk(k)G(k),k=0,1,....,255

where N = total no. of pixels, β(k) = cut-off function

if (Tk255-T):
    k=1
else:
    k=0

Where T = cut-off frequency

• Step 3. We then verify F with threshold η, and if F is greater than η, then we conclude contrast enhancement has been applied.

Choosing the cut-off frequency T is very important in this algorithm. A large T will only take a small fraction of the high frequencies which will make the model oversensitive. While a small T value will increase the number of flagged frequencies causing accuracy to decrease. [6]

1.3 Proposed technique in [7]:

This paper, [7], proposes a contrast enhancement detection technique based on zero-height gap bin of the histogram. Zero-height gap bin is a bin in the histogram where there is no frequency or in plain terms where there is a gap in the histogram. It is a common thing observed in tampered images. [7]

The steps are given ahead. This paper did conclusive experimental analysis to find that the contrast enhancement detector model achieved high performance. [7]

4.2 Benford's law:

Another image property which is related to detecting contrast is the Discrete Cosine Transform (DCT). The authors of [9] proposes a method which utilizes DCT using an important concept in statistics: Benford's Law. Benford's law tells us the distribution of each digit in numerical data, where each digit follows a logarithmic law which can be used to predict the most significant digit appearing next in naturally occurring data. Benford's law is stated as:

1) Compute the normalized grey level histogram h(x) of the image.

2) Check which bin exists at zero-height gap based on function:

h(k)=0,

min{h(k-1), h(k+1)}> τ

121+1 x=k-1k+1h(x)>τ

3) Use the decision threshold 'τ' to determine if contrast enhancement is detected. If Ng, the number of zero-height gap bins is more than τ, then we conclude contrast enhancement is detected.

p(d) = $\log_{10}$(1+1d) where d is the digit.[9]

DCT is said to follow Benford's law and hence can be used to detect contrast image forgery. The system model for the proposed idea is as follows: [9]

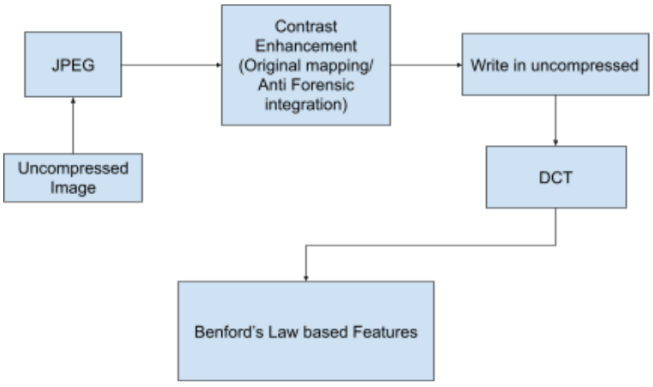


Fig -5: System Model for extraction of Benford's law based features.

As mentioned before, DCT follows Benford's law, so the test case used by this paper was fitted with a chi-square divergence on Benford's distribution and the mean Chi-

Square divergence for unaltered image came out to be 0.0034 and for altered image it came out to be 0.0180. This is quite a significant difference, and hence can be used for contrast enhancement detection. [9]

5. SVM

SVM stands for Support Vector Machine. SVM is a supervised machine learning algorithm that can be used for both regression and classification purposes. [15]
Its major usage lies in classification problems. SVM classifier is used in several areas to find forgery in an image. The method is used to find similar regions of images by matching image blocks and identifying the regions that have been tampered or changed.
This technique comprises two techniques, namely, the training phase and the testing phase. The training phase involves the SVM trained by a set of images. SVM will primarily identify the decision boundaries in the training phase and then the technique provides efficient generalization in high dimensional input images. Classification using SVM is mainly based on decision making which defines the decisional boundaries. SVM determines a vector called 'support vector.' These identify the separators that can classify the wide separation of classes and objects. SVM supports binary and multiclass targets. The models must have similar functional forms for block based and radial basis functions. The SVM maps original data points from input image to high dimensional feature block making classification problems simpler in feature space. [18]
The SVM classification model is based on geometric properties. This makes it appropriate for usage in off-line verification problems where the features are static in nature. [15]
In terms of forgery detection, the SVM can be used in several different techniques that could be able to find the tampering and changes in images. Several researchers have proposed their own modifications to the traditional usage of SVM Classifier to develop their own methods of detecting forgery in images.
As proposed by Reshma P.D. and Arunvirodh C in [17], for the purpose of Image Forgery Detection, the technique highlights the use of illuminant color inconsistency for forgery detection. They have proposed the following steps for their method:

1. Illuminant color estimation: Using the gray world algorithm, a new image is created in which each area is colored with the color of the extracted illuminant color, which is called an illuminant map.
2. Face extraction: The faces in the image that are to be investigated are to be extracted. This is done by the use of a face detector using the vision toolbox wherein all the faces present in the image are extracted.
3. Feature extraction: Different images require different techniques to perform feature extraction. Herein, there were three main features that were extracted for good performance, namely SIFT (Scale Invariant Feature Transform), HOG (Histogram of Oriented Gradients) and GLCM (Gray Level Concurrence Matrix) features.
4. Classification: SVM classifier is used since it is theoretically superior machine learning, with great results for high-dimensional datasets. Classifier checks the features and accurately classifies the image on the basis of its originality.

In the proposed work [18] by Dr. Palanivel .N, Arthi .Z, Deepika .G and Latha .S, gives the technique to find a duplicate region in an image by the usage of PCA algorithm and SVM Classifier in the following steps:

1. Dividing the grayscale image into fixed size overlapping blocks using SVM.
2. Extracting Gaussian RBF kernel PCA-based features from each DCT square block.
3. Matching similar block pairs.
4. Removing the isolated block and outputting the duplicated regions.

6. CONCLUSIONS

We have presented a review of the different methods that can be used for image forgery detection. These techniques are widely used and modified in several areas for identification of tampering in the image. The organization of this work has enabled us to understand the different references and serve it as a source for reference.
Our work has provided us an opportunity to read and understand various methods of image forgery detection. Since different types of forgery require different methods of identification, we focused on the copy-move forgery detection techniques which mainly included Key-Point matching technique and Block based matching technique, the different algorithms that showed how color schemes and patterns identified forgery as well as the usage of SVM classifier in the detection. We covered several aspects of these techniques and different usages and interpretations of the same.
Finally, we hope that this paper can contribute to development of new ideas and information gain on these techniques, in the field of image forgery detection, which would directly benefit the image forensics domain.

REFERENCES

[1] Kasban, H., & Nassar, S. (2020). An efficient approach for forgery detection in digital images using Hilbert Huang transform. Applied Soft Computing, 106728.
[2] Azad, Dr & Hasan, Md & K, Mohammed. (2017). Color Image Processing on Digital Image. International Journal of New Technology and Research. 3. 56-62.
[3] Huang, S., Cai, N., Pacheco, P. P., Narrandes, S., Wang, Y., & Xu, W. (2018). Applications of Support Vector Machine

(SVM) Learning in Cancer Genomics. Cancer genomics & proteomics, 15(1), 41–51.

[4] Copy move forgery detection using key point localized super pixel based on texture features C. Rajalakshmi 1 , M.G. Alex 1,2, R. Balasubramanian 1,3

[5] DETECTING MULTIPLE COPIES IN TAMPERED IMAGES E. Ardizzone, A. Bruno, G. Mazzola Dipartimento di Ingegneria Informatica (DINFO) dell'Università di Palermo. Viale delle Scienze – Ed. 6, 90128, Palermo, Italy

[6] Two Improved Forensic Methods of Detecting Contrast Enhancement in Digital Images Xufeng Lin, Xingjie Wei and Chang-Tsun Li

[7] Contrast Enhancement-Based Forensics in Digital Images Gang Cao, Yao Zhao, Senior Member, IEEE, Rongrong Ni, Member, IEEE, and Xuelong Li, Fellow, IEEE

[8] Detection of Contrast Enhancement Forgery in Previously and Post Compressed JPEG Images, 2019 5th International Conference for Convergence in Technology (I2CT) Pune, India. Mar 29-31, 2019

[9] Benford's Law for Detecting Contrast Enhancement Syeda Shira Moin, Saiful Islam

[10] Toqeer Mahmood, Tabassam Nawaz, Rehan Ashraf, Mohsin Shah, Zakir Khan, Aun Irtaza, Zahid Mehmood," A survey on block based copy move image forgery detection techniques" International Conference on Emerging Technologies (ICET) - 2015

[11] Shibu S. Narayanan; G. Gopakumar "Recursive Block Based Keypoint Matching For Copy Move Image Forgery Detection" 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) - 2020

[12] Priyanka Arora, Derminder Singh "Copy Move Image Forgery Detection with Exact Match Block Based Technique" Oriental Journal of Computer Science and Technology- 2019

[13] Malti Puri ,Dr. Vinay Chopra "A review block-based copy move forgery detection methods" International Journal of Engineering Research & Technology (IJERT)-2016

[14] Chanop Silpa-Anan, Richard Hartley; "Optimised KD-trees for fast image descriptor matching" ;IEEE -2008

[15] Seung-Jin Ryu, Hae-Yeoun Lee, Il-Weon Cho, and Heung-Kyu Lee. 2008. Document Forgery Detection with SVM Classifier and Image Quality Measures. In Proceedings of the 9th Pacific Rim Conference on Multimedia: Advances in Multimedia Information Processing (PCM '08). Springer-Verlag, Berlin, Heidelberg, 486–495. DOI:https://doi.org/10.1007/978-3-540-89796-5_50

[16] L. E. Martinez, C. M. Travieso, J. B. Alonso and M. A. Ferrer, "Parameterization of a forgery handwritten signature verification system using SVM," 38th Annual 2004 International Carnahan Conference on Security Technology, 2004., 2004, pp. 193-196, doi: 10.1109/CCST.2004.1405391.

[17] Reshma P.D and Arunvinodh C, "Image forgery detection using SVM classifier," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1-5, doi: 10.1109/ICIIECS.2015.7193202.

[18] Dr Palanivel .N, Arthi.Z, Deepika.G, Latha.S, "Image forgery detection using support vector machine", International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 03 | Mar 2019.

[19] George Jiji,Detecting Digital Image Forgeries using Color Constancy,International Journal of Scientific & Engineering Research, Volume 5, Issue 10, October-2014.